UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/931,794	08/16/2001	William L. Jones	002.0221.01	3670

22895 7590 03/07/2005

PATRICK J S INOUYE P S
810 3RD AVENUE
SUITE 258
SEATTLE, WA 98104

EXAMINER	
SCHUBERT, KEVIN R	
ART UNIT	**PAPER NUMBER**
2137	

DATE MAILED: 03/07/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/931,794	JONES, WILLIAM L	
	Examiner	Art Unit	
	Kevin Schubert	2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *16 August 2001*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-72* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-72* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *16 August 2001* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date *10222001*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Claims 1-72 have been considered.

Claim Rejections - 35 USC § 112

The following is a quotation of the first paragraph of 35 U.S.C. 112:

> The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

Claims 35,41,47,52,58,62,67, and 70 are rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the enablement requirement. The claim(s) contains subject matter which was not described in the specification in such a way as to enable one skilled in the art to which it pertains, or with which it is most nearly connected, to make and/or use the invention.

The claims describe the use of a public key as the encryption key for a digital signature and a private key as the decryption key. It is commonly known in the art that a digital signature is based on a user signing a hash with his privately held private key. The general public can then verify that the user is who he says he is through the publicly known public key. Furthermore, the applicant writes, "To verify digitally signed video content... a private key is used as the encryption key and a public key is used as the decryption key" (Specification page 9). Since the applicant suggests that he is using the commonly known standard of creating a digital signature, the claims have been rejected for not being enabled.

Claims 48 and 53 are rejected under 35 U.S.C. 112, first paragraph for being dependent on claim 47. Since claim 47 is not enabled, neither is claim 48.

Claim Rejections - 35 USC § 112

The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

Claims 1,7,10,16,20,24,26,30,33,34,37,39,43,46,51,57,59,61,63,66, and 69 are rejected under 112 2nd paragraph. The term "substantially" as used in the phrases "substantially identical" and "substantially continuous" in the above claims is a relative term which renders the claims indefinite. The term "substantially" is not defined by the claim, the specification does not provide a standard for ascertaining the requisite degree, and one of ordinary skill in the art would not be reasonably apprised of the scope of the invention.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 1,4-10,13-20,23-26,29-33,36-39, and 42-45 are rejected under 35 U.S.C. 103(a) as being unpatentable over Matsushita, EP Patent Application No. EP 1,096,714 A2, in view of Jones, U.S. Patent No. 5,623,637.

As per claims 1,10,20,26,33, and 39, the applicant describes a system for automatically protecting private video content using cryptographic security for legacy systems comprising the following limitations which are met by Matsushita in view of Jones:

a) recording logic intercepting a substantially continuous video signal representing video content in the process of being recorded on a transportable storage medium (Matsushita: Col 3, lines 25-52; 51 of Fig 4);

b) a frame buffer dividing the intercepted substantially continuous video signal into individual frames during recording, each individual frame storing a fixed amount of data in digital form, and combining decrypted frames into a substantially continuous video signal during playback (Matsushita: Col 3, lines 25-52; 53 of Fig 4);

c) a processor encrypting each individual frame into encrypted video content using an encryption cryptographic key and storing the encrypted frames during recording and retrieving the encrypted frames and decrypting each encrypted frame using a decryption cryptographic key during playback (Matsushita: Col 3, lines 25-52; 54 of Fig 4);

d) reading logic outputting the substantially continuous video signal as video content in the process of being played from the transportable storage medium (Matsushita: Col 3, lines 25-52; 55 of Fig 4);

Matsushita describes an encryption control apparatus which receives content data, such as video data, from a device such as "portable information equipment" (Col 9, lines 51-52) or a video recorder and frames, encrypts, and stores the received information to a memory card (Col 9, line 46 to Col 10, line 4). When the information is reproduced, such as during playback, the encryption control apparatus decrypts the frames one by one through the extraction unit and combines the decrypted frames with their appropriate headers as output. Matsushita describes all the limitations of parts a) through d) of the above claim.

However, Matsushita fails to disclose that his system takes place on transportable storage medium such as the memory card itself. Since Matsushita's system fails to take place on transportable storage medium, it is not suitable for legacy systems. Jones describes a system similar to Matsushita's in which a unique memory card accepts data which is intended to be written to the memory card and automatically encrypts the data for storage. When the data is to be read, such as during playback of the content, the data is decrypted by a decryption key upon the user supplying appropriate credentials (Jones: Col 6, lines 5-21). Furthermore, Jones' unique memory card satisfies the applicant's limitation of being suitable for legacy systems because the unique memory card can be used with a legacy system since the legacy system does not need to be altered.

Implementing the ideas of Matsushita's encryption control apparatus in Jones' system is easily done by replacing the Encrypt-Decrypt module of Jones (177 of Fig 1) with the Encryption Control module of Matsushita (50 of Figs 3 and 4). Also, Jones' processor (Jones 260 of Fig 1; Col 6, lines 11-14) which controls the Encrypt-Decrypt module would now control the Encryption Control module. It would have been obvious to one of ordinary skill in the art at the time the invention was filed to incorporate Matsushita with the ideas of Jones because Jones merely describes the encryption and decryption of data and Matsushita describes a special way of encrypting and decrypting data (extracting frames of data and encrypting the individual frames) which is the typical way video and audio content is processed and stored. Thus, when audio-video data is being recorded onto the memory card of Jones' system, it would be appropriate to frame the data and encrypt the individual frames for storage.

As per claims 4 and 13, the applicant describes the system according to claim 1 (etc), which is met by Matsushita in view of Jones (see above), with the following limitation which is met by Jones:

A validation module validating the decryption cryptographic key against user-provided credentials prior to decrypting the encrypted frames (Jones: Col 8, lines 52-63).

As per claims 5,14,23,29,36, and 42, the applicant describes the system according to claim 1 (etc), which is met by Matsushita in view of Jones (see above), with the following limitation which is met by Jones:

An asymmetric cryptographic key pair comprising a public key corresponding to the encryption cryptographic key and a private key corresponding to the decryption cryptographic key (Jones: Col 6, lines 5-10; Col 1, lines 41-49);

Jones discloses that the encryption/decryption key algorithm is "preferably...symmetrical key algorithm" (Col 6, line 8). Since the two types of encryption algorithms are symmetrical and asymmetrical, Jones also leaves the system open to asymmetric key cryptography. Furthermore, Jones discusses the use of asymmetric key cryptography, in particular the RSA algorithm, as a means of encryption/decryption (Col 1, lines 41-49).

Combining Jones with his disclosure in the prior art and his implication that asymmetric key cryptography can be used in the system, the encryption/decryption module can encrypt the content with a public or private key obtained in the EEPROM (257 of Fig 1) of the smartcard IC and decrypt the content with the corresponding public or private key obtained from the EEPROM when the content is being decrypted.

As per claims 6 and 15 the applicant describes the system according to claim 5 (etc), which is met by Matsushita in view of Jones (see above), with the following limitation which is met by Jones:

Wherein the asymmetric cryptographic key pair comprises at least one of an RSA-compatible key pair, a TwoFish-compatible key pair and a Diffie-Hellman-compatible key pair (Jones: Col 1, lines 41-49).

As per claims 7,16,24,30,37, and 43, the applicant describes the system according to claim 1 (etc), which is met by Matsushita in view of Jones (see above), with the following limitation which is met by Jones:

A symmetric cryptographic key pair comprising a substantially identical key corresponding to each of the encryption cryptographic key and the decryption cryptographic key (Col 6, lines 5-10).

As per claims 8,17,25,31,38, and 44, the applicant describes the system of claim 1 (etc), which is met by Matsushita in view of Jones (see above), with the following limitation which is met by Jones:

A removable storage medium storing at least one of the encryption cryptographic key and the decryption cryptographic key (Jones: Col 6, lines 5-10);

The removable storage medium is the memory card which has the smartcard IC on it which stores the encryption and decryption cryptographic keys in its EEPROM.

As per claims 9 and 18 the applicant describes the system of claim 8 (etc), which is met by Matsushita in view of Jones (see above), with the following limitation which are met by Jones and Matsushita:

A set of cryptographic instructions stored on the removable storage medium and employing at least one of the encryption cryptographic key and the decryption cryptographic key (Jones: Col 6, lines 5-10; Matsushita Col 3, lines 25-52);

Both Jones and Matsushita disclose encryption/decryption modules which contain instructions for encrypting and decrypting a set of data.

As per claims 19,32, and 45, the applicant describes the method according to claims 10,11,12,13,14,16,17, or 18 (etc), which are met by Matsushita in view of Jones (see above), with the following limitation which is met by Jones:

A computer readable storage medium holding code for performing the method of claims 10,11,12,13,14,16,17, or 18 (Col 2, lines 10-22);

The computer readable storage medium is a memory card in the preferred embodiment which inherently contains code to execute the encryption/decryption method of the system.

Claims 2-3,12,21-22,27-28,46,48-50,57,59-61, and 63-65 are rejected under 35 U.S.C. 103(a) as being unpatentable over Matsushita in view of Jones in further view of Friedman, U.S. Patent No. 5,499,294.

As per claims 2,21, and 27, the applicant describes the method according to claim 1 (etc), which is met by Matsushita in view of Jones (see above), with the following limitation which is anticipated by Friedman:

An authentication module generating a fixed-length original cryptographic hash from at least one such individual frame, encrypting the original cryptographic hash using an encryption cryptographic key, storing the encrypted original cryptographic hash as a digital signature on a transportable storage medium, decrypting the encrypted original cryptographic hash using a decryption cryptographic key, generating a verification fixed-length cryptographic hash from at least one such individual frame, and

comparing the verification cryptographic hash and the original cryptographic hash (Friedman: Col 4, line 63 to Col 5, line 14; Col 5, lines 49-65);

Matsushita in view of Jones describes all the limitations of claims 1, 20, and 27. However, Matsushita in view of Jones fails to describe an authentication module for verifying the authenticity of the data.

Friedman describes a video camera system, similar to that of the Friedman and Matsushita, in which individual image frames are hashed, a digital signature is created for the image frames, and the digital signature is stored with the image frames so that authenticity can be proven when desired.

It would have been obvious to one of ordinary skill in the art at the time the invention was filed to incorporate the ideas of Friedman with those of Matsushita in view of Jones for the purpose of authenticating data on the memory card so that encrypted stored data can be verified when it is decrypted in order to prove that the data has not been tampered with since storage.

Incorporating Friedman into the system of Matsushita in view of Jones would be easy. The authentication module would be comprised of two parts and would be positioned immediately left of the Encryption Control unit. The first part would be implemented when data is received from the host computer and would create a digital signature, store the digital signature, and transmit the normal image file to the Encryption Control Unit. The first part would be comprised of Fig 3B of Friedman. The second part, Fig 3C of Friedman, would be implemented when data is received from the Encryption Control Unit and would retrieve the digital signature, decrypt the digital signature, calculate a new hash, and compare the new hash with the decrypted digital signature to check for authenticity.

As per claims 3,12,22, and 28, the applicant describes the system according to claim 2 (etc), which is met by Matsushita in view of Jones in further view of Friedman (see above), with the following limitation which is met by Jones and Friedman:

An asymmetric cryptographic key pair comprising a private key corresponding to the encryption cryptographic key and a public key corresponding to the decryption cryptographic key (Jones: Col 6, lines 5-10; Col 1, lines 41-49; Friedman: Abstract);

Both Jones and Friedman discuss the use of asymmetric cryptography.

As per claim 46, the applicant describes a method for automatically authenticating private video content using cryptographic security for legacy systems in which parts a), b), and d) have been previously discussed as rejected under Matsushita in view of Jones (see rejection for claim 1) and part c) has been previously rejected under Friedman (see rejection for claim 2).

As per claims 48-50, the applicant describes the limitations of claim 6,8,9 respectively and are rejected for the same reasons as claims 6,8, and 9 but are now rejected under Matsushita in view of Jones in further view of Friedman rather than Matsushita in view of Jones.

As per claim 57, the applicant describes a system for digitally signing private video content using cryptographic security for legacy systems comprising parts a) and b) which are rejected under Matsushita in view of Jones as previously discussed (see claim 1) and part c) which is rejected under Friedman (see claim 2).

As per claims 59 and 60, the applicant describes the limitations of claims 7 and 8 and are rejected for the same reasons as claims 7 and 8 but are now rejected under Matsushita in view of Jones in further view of Friedman rather than Matsushita in view of Jones.

As per claim 61, the applicant describes a method for digitally signing private video content using cryptographic security for legacy systems comprising parts a) and b) which are rejected under Matsushita in view of Jones as previously discussed (see claim 1) and parts c),d), and e) which are rejected under Friedman (see claim 2).

As per claims 63-64, the applicant describes the limitations of claims 7 and 8 respectively and are rejected for the same reasons as claims 7 and 8 but are now rejected under Matsushita in view of Jones in further view of Friedman rather than Matsushita in view of Jones.

As per claim 65, the applicant describes the limitation of claim 19 and is rejected for the same reasons as claim 19 but is now rejected under Matsushita in view of Jones in further view of Friedman rather than Matsushita in view of Jones.

Claims 11,34,40,51,53-56,66,68-69, and 71-72 are rejected under 35 U.S.C. 103(a) as being unpatentable over Matsushita in view of Jones in further view of Friedman in further view of Yokota, U.S. Patent Application Publication No. 2003/0120604.

As per claims 11,34, and 40, the applicant discloses the method of claim 10 (etc), which is anticipated by Matsushita in view of Jones (see above), with the limitation of generating a cryptographic hash and comparing it with an original hash which is anticipated by Friedman (see the rejection for claim), and the following additional limitations which is met by Yokota:

e) outputting the substantially continuous video signal upon successful comparison of the verification cryptographic hash and the original cryptographic hash (Yokota: [0571] and [0572]);

Matsushita in view of Jones in further view of Friedman discloses all the limitations of the above claim except for sending the video signal based on the comparison.

Yokota discloses the idea of only reproducing data if a successful hash comparison reveals that the data is authentic. It would have been obvious to one of ordinary skill in the art at the time the invention was filed to incorporate the ideas of Yokota with those of Matsushita in view of Jones in further view of Friedman and only reproduce the data if the comparison which takes place in the authentication module of Friedman reveals the data is authentic because unauthentic data may have been manipulated by a hacker.

This implementation would be easy. It would just require that the decrypted content which passes through the authentication module is sent to the host computer only if the comparison reveals the data is authentic.

As per claims 51,66, and 69, the applicant describes a method for automatically authenticating private video content using cryptographic security for legacy systems comprising parts a),b), and g) which are met by Jones in view of Matsushita (see rejection for claim 1), parts c),d),e), and f) which are met by Friedman (see rejection for claim 2), and part g) which is met by Yokota (see rejection for claim 11).

As per claims 53-55, the applicant describes the limitations of claims 6,8,9 respectively and are rejected for the same reasons as claims 6,8, and 9 but are now rejected under Matsushita in view of Jones in further view of Friedman in further view of Yokota rather than Matsushita in view of Jones.

As per claims 56 and 72, the applicant describes the limitation of claim 19 and the claims are rejected for the same reasons as claim 19 but are now rejected under Matsushita in view of Jones in further view of Friedman in further view of Yokota rather than Matsushita in view of Jones.

As per claims 68 and 71, the applicant describes the limitation of claim 8 and the claims are rejected for the same reasons as claim 8 but are now rejected under Matsushita in view of Jones in further view of Friedman in further view of Yokota rather than Matsushita in view of Jones.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Kevin Schubert whose telephone number is (571) 272-4239. The examiner can normally be reached on M-F 8:00-5:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Andrew Caldwell can be reached on (571) 272-3868. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

***

Andrew Caldwell

ANDREW CALDWELL
SUPERVISORY PATENT EXAMINER